UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,704	08/09/2001	Jerome Anthony Solinas	SOLINAS-3	6759

7590 01/13/2005

ATTN: PATENT COUNSEL, OGC
NATIONAL SECURITY AGENCY
STE 6542
9800 SAUAGE ROAD
FT MEADE, MD 20755-6542

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/928,704	SOLINAS, JEROME ANTHONY	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the c ver sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08/09/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 1 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over copending Application No. 09/928,266 (hereinafter referred to as *Solinas*) in view of US Patent 5,271,061 (hereinafter referred to as *Crandall).*

As per claim 1, *Crandall* discloses a method of exchanging a cryptographic key between two users, comprising the steps of:

a) selecting, by a recipient, a modulus p from an equation (see column 7 lines 23-27);
b) each of said two users selecting an elliptic curve E and an order q (see column 7 lines 10-33);
c) each of said two users selecting a base point G=(Gx, Gy) on the elliptic curve E where G is of order q (see column 7 lines 38-41);
d) each of said two users generating a private key w, where w is an integer (see column 7 lines 18-21);
e) each of said two users generating a public key W=wG, where W is the corresponding user's public key, where w is the corresponding user's private key, and where G is the corresponding user's basepoint (see column 8 lines 6-15);
f) each of said two users distributing their p, E, q, G, and W in an authentic manner (see column 8 lines 16-17 and column 7 lines 23-33);
g) the two users agreeing on p, E, q, G, W_1 and W_2, where W_1 is the public key of one of said users, and where W_2 is the public key of the other of said two users (see column 8 lines 16-17 and column 7 lines 23-33);
h) each of said two users generating a private integer (see column 7 lines 18-21);
i) each of said two users multiplying G by each of said user's private integer generated in the last step using a form of p agreed upon (see column 8 lines 6-15);
j) each of said two users transmitting the result of the last step to the other of said two users (see column 8 lines 16-17);
k) each of said two users combining, one of said two user's private integer and public key with the other of said two user's result of step (j) and public key using the form of p agreed upon to form a common secret point between each of said two users (see column 8 lines 24-28);
l) each of said two users deriving the cryptographic key from the common secret point (see column 8 lines 24-28 and 38-42);

Crandall fails to mention the selection of a modulus p from a group of equations consisting of:

$p = (2^{dk} - 2^{ck} - 1)/r$,
where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$;
$p = (2^{dk} - 2^{(d-1)k} + 2^{(d-2)k} - \ldots - 2^{k} + 1)/r$,
where d is even, and where k is not equal to 2 (mod 4);

$p = (2^{dk} - 2^{ck} - 1)/r,$
where $3d<6c<4d$, and where GCD(c,d)=1;
$p = (2^{dk} - 2^{ck} + 1)/r,$
where $0<2c<=d$, where r /= 1, and where GCD(c,d)=1;
$p = (2^{4k} - 2^{3k} + 2^{2k} + 1)/r,$

Solinas describes the abovementioned selection of modulus p in his detailed description (see pages 17-18).

It would have been obvious to a person of average skill in the area at the time of the invention to include within the *Crandall* cryptographic system *Solinas'* equations in order to decrease the number of steps necessary.

This is a provisional obviousness-type double patenting rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER